Linksys WAP54G Hardware Spec

Contents

Installation

WARNING - DD-WRT was not originally intended to be loaded on a WAP unit. It was found that it will run but it is a tricky unit to load and have function correctly. Below are a compilation of methods/instructions to assist you with creating a DD-WRT-loaded WAP unit. LOAD AT YOUR OWN RISK.
Hard reset does not work on this device, so it is not possible to clear NVRAM using the reset button. This can be problematic if a reset is required to access it. If this happens, reinstall the Linksys firmware using the tftp method, then reset it.

MAC ADDRESS CHANGES

If you really want your WAP to have the correct MAC address when it boots up there are 2 methods....one simple but not permanent, and one not so simple but permanent.

Method 1

For V1.x only

On the *Administration->Commands* tab enter:

```
nvram set et1macaddr=<your MAC address minus 1 here> (due to the port swap) (i.e. 00:11:22:33:44:
nvram commit
```

Run then Save as Startup....now reboot the unit for the new MAC to take effect.

For V2 units - This unit version has a unique motherboard flag and should be recognized as a WAP on the Status tab.

For MAC alterations on a V2.0- V3.x - follow the same step above except substitute the et1macaddr with et0macaddr and don't use the minus 1, use your actual MAC address. (i.e. 00:11:22:33:44:55)

This will need to be re-entered if you do a hard reset (like when doing firmware upgrades).

Example of startup script for a V1:

```
nvram set et1macaddr=00:11:22:33:44:54
nvram set boardnum=2
nvram commit
```

Example of startup script for a V2.0:

```
nvram set et0macaddr=00:11:22:33:44:55
nvram commit
```

Example of startup script for a V3.X:

```
nvram set et0macaddr=00:11:22:33:44:55
nvram set WAPver=3
nvram commit
```

Run the script and save as Startup, then power cycle. It should then be recognized as a WAP unit on the status tab.

Method 2

This works for all WAPs (For v2.0 and v3.X use actual MAC and MAC+1)

Extract your CFE, edit in your MAC address, et0macaddr = MAC, and il0macaddr=MAC+1. (For V1.x... Use your MAC-1 for the lan_hwaddr and your MAC for the wan_hwaddr), then put the CFE back on using the HairyDairyMaid or TJTAG utility. This method is risky. You could potentially turn your router into a brick. Once this is reinstalled on the unit and the firmware has been loaded, your unit will have its own MAC addresses permanently embedded and will show every time you boot.

[note] - for the V1s, search for the embedded text string "hwaddr" using your hex editor. This will find the two MAC addresses that are embedded. Again due to the port swap the LAN MAC address needs to be entered as MAC-1 and wan_hwaddr needs to be entered as the MAC for the V1.X only

[note] - my WAP 1.0 required 192.168.1.1 using tftp.exe for the firmware load the first time... my V2.0 and 3.1 required 192.168.1.245 using tftp.exe for the firmware load the first time.

Firmware Install

WARNING - Use only Micro builds on the WAP54G units. The micro_special_generic.bin (e.g. 36247) has been indicated to work on the v1.x, but is unknown on the v2.0 and v3.x (which can use e.g. 14929 or 36247.)

WAP54G v1.X

- Has fixed LED displays starting with V24 RC5. - redhawk - Builds earlier than Dec/17/2017 are vulnerable to WPA2 KRACK - liverpoolatnight

- Connect PC to LAN port on WAP
- Configure PC for STATIC IP as 192.168.1.2 Mask 255.255.255.0, Gateway 192.168.1.245
- Perform a 30/30/30 hard reset
- Open Browser, URL = http://192.168.1.245
- Login as: Username/Password <blank>/admin
- Navigate to Administration Tab. **Change the DD-WRT micro_special_generic.bin file to xxx_generic.trx**
- Upload the new xxx_generic.trx file to the router.
- Wait 5 minutes after it says it completes successfully.
- Unplug WAP unit, plug it back in.
- Perform a 30/30/30 hard reset
- Now use URL = http://192.168.1.1
- Go to the *Administration->Commands* tab
- Enter the following:

```
nvram show | grep boardnum
```

- If *boardnum=2* **is not returned**, then enter this and click *Run Commands':*

```
nvram set boardnum=2
nvram commit
```

- Click "Run" button and then: "Save Startup" button. - (only if you had to enter boardnum=2 manually)
- Power cycle the WAP unit.
- Check the Status page... it should now display the unit as a "Linksys WAP54G v1.x"
- Configure as you would any other router.

Power = Power, Diag = Diag or Commit

WLAN - **Link LED is now a Radio On/Off indicator**, Act = Wireless Activity

LAN - Link = Link, Full/Col = Full, 100 = 100

Thanks goes to Eko for making this unit display correctly.

WAP v2.0

Follow the steps for the WAP v3.x below but exclude the nvram variable for 'WAPver=3'. The v2 units have a unique board and should be already recognized by the RC5 and later firmware. Eko said no special variables are needed for the v2 [redhawk]

NOTE: On my V2.0 unit, it has original 2.07 Linksys firmware installed... this FW would not upgrade to DD-WRT. I first downloaded the latest 3.04 FW from the Linksys site and upgraded to it first. Then it would accept the DD-WRT micro_generic build (renamed to .trx extension) directly from the web GUI in the Linksys pages.

If you receive a error message saying "Unable to downgrade firmware" go to http://192.168.1.245/fw-conf.asp, set pull-down menu "DownGrade Header :" to disable and click [apply]. If this setting executed successful you see a message "Your changes have been saved". [ddvelzen - 18/01/08]

- I have also included an updated DD-WRT FW due to the vulnerable KRACK, I have tryed this myself and tested with **r35927** see https://imgur.com/a/A0hgCzj [liverpoolatnight 14/July/2018]

WAP54G v3.X

Use V24-RC5 or later for Reset button function

- Connect PC to LAN port on WAP
- Configure PC ethernet port to *IP: 192.168.1.2, SM: 255.255.255.0, GW: 192.168.1.245*
- Powerup the router, then perform a 30/30/30 hard reset on it
- Open your favorite browser (I used Firefox) and go to: **http://192.168.1.245**
- Login using:
    - **User:** <blank>
    - **Password:** admin

Go to the Administration tab and upload the MICRO firmware.

- Wait 5 minutes after it says it completes successfully.
- Perform a 30/30/30 hard reset
- Open *http://192.168.1.1* in your browser and login with the default DD-WRT user/password
- Go to the *Administration->Commands* (or see Telnet section below)
- Type in the following '*only for v3.x WAP units': do not use on a v2.0 unit* (with V24-RC5 and later firmware)

'*NOTE: review the* MAC ADDRESS CHANGES**section, in case the *et0macaddr* needs added too**

```
nvram set WAPver=3
nvram commit
```

IT IS VERY IMPORTANT TO USE THESE COMMANDS ON A V.3.X UNIT OR YOU WILL LOSE THE RESET BUTTON!

- Click on "Run Commands" and wait for it to return without error. Some builds don't handle the Commands properly.

    - ♦ It was once noted to also save to "Startup" but many report this resets nvram, plus a reset removes Startup anyway.
- Reboot the router then configure.

If you did NOT set the WAPver=3, and are now locked out of your router, try these instructions from Redhawk0 to get your router working again, and then set the instructions set out above:

- use tftp.exe program....but use the default linksys address to flash it again with a micro_generic.bin file.
- use tftp at 192.168.1.245 to talk to the unit....set a static IP on your computer first to 192.168.1.10
- Follow the tftp flash instructions in the peacock thread...but use 1.245 for the WAP address.

If the firmware update on a WAP54G v3.1 gives an "upgrade failed" message, perform a 30/30/30 hard reset then try to TFTP the micro build as above.

For trouble reconnecting after firmware upgrade, the arp table could be caching the old MAC address. Try:

```
netsh interface ip delete arpcache
```

Reference: this forum post.

IMPORTANT: DD-WRT firmware will turn these units into NAT routers, similar to a 2MB flash WRT54G. However, the wireless interface and the ethernet interface are reversed. The firmware considers the wireless interface the WAN interface, and the ethernet interface the LAN interface. Thus, you cannot substitute one of these units for a regular WRT54G in NAT mode. ' You CAN use it as a gateway router, routing between subnets with NAT switched off, or as an access point, or as a LAN-to-wireless bridge.

- Reverse it by changing the WAN port assignment.
- Go to *Setup -> Networking -> Port Setup*
- Change the WAN port assignment twice: first to br0, and then change it again to vlan0.
- Now the ethernet is the WAN, and wireless is the LAN.

Unbrick via Pin Short

This is not recommended. If TFTP fails to work with no pings received at powerup, and the power and link LEDs are stuck on, a pin short can be tried for unbricking. Short the flash memory pins 15 & 16 using the Linksys WRT54G Revival method. Tested on a WAP54G v3.1: locate the flash memory located on the circuit board bottom. Shorting the pins with a paperclip should enable pings and web interface access.

Telnet for WAPver

Use these commands, noting the quotation marks, and each line ends with enter:

```
nvram set WAPver=3
nvram rc_startup="nvram set WAPver=3
nvram commit"
nvram commit
reboot
```

WAP54G v2.0 Serial Header

- Serial: J5
- JTAG: CONN1